In the Claims:

Please amend claims 2, 5, and 6. The claims are as follows:

1. (Previously presented) A method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and

verifying by the browser the SCAC certificate using a new public key of the certifying authority.

2. (Currently amended) The method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

verifying the request by the certifying authority using the server's public key; and

generating the SCAC certificate by the certifying authority using ~~it's~~ a new private key of

PAGE 3/12 * RCVD AT 10/5/2004 10:22:08 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-24

the certifying authority and forwarding the SCAC certificate to the server.

3. (Previously presented) The method of claim 2 wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

4.(Previously presented) The method of claim 1, further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

5. (Currently amended) The method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake.

6. (Currently amended) In an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising:

[[a]] means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority,

[[a]] means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,[[,]]

PAGE 4/12 * RCVD AT 10/5/2004 10:22:08 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-24

[[a]] means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser.

7-10. (Canceled)

11. (Previously presented) The method of claim 1, further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate.

12. (Previously presented) The method of claim 1, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority.

13. (Previously presented) A system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

means for receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

means for verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and

PAGE 5/12 * RCVD AT 10/5/2004 10:22:08 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-24

means for verifying by the browser the SCAC certificate using a new public key of the certifying authority.

14. (Previously presented) The system of claim 13, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

means for contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

means for verifying the request by the certifying authority using the server's public key; and

means for generating the SCAC certificate by the certifying authority using it's a new private key of the certifying authority and forwarding the SCAC certificate to the server.

15. (Previously presented) The system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

16. (Previously presented) The system of claim 15, further comprising means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

PAGE 6/12 * RCVD AT 10/5/2004 10:22:08 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-24

17. (Previously presented) The system of claim 13, wherein the system further comprises means for presenting the CCAC certificate to the server during the handshake.

18. (Previously presented) The system of claim 13, further comprising means for accepting the transaction by the browser in conjunction with said means for verifying the original authentication certificate and in conjunction with said means for verifying the SCAC certificate.

19. (Previously presented) The system of claim 13, wherein said means for obtaining the SCAC certificate comprises use of the new private key of the certifying authority.

PAGE 7/12 * RCVD AT 10/5/2004 10:22:08 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-24